Aligning IT risk management with the enterprise through effective KRI's
Organizations are facing an increasing challenge from regulators, investors, and auditors to define their risk appetite. Technology is a key driver in enabling business, so it is imperative for management to consider technology in its definition of risk. Management is starting to focus on determining enterprise risk appetite and measuring adherence to it, but has paid too little attention to how their IT systems affect risk appetite. The reason? Challenges choosing and applying appropriate IT key risk indicators (KRIs).

KRIs are metrics that demonstrate the risks that an organization is facing. They are the mainstay of measuring adherence to and establishing enterprise risk appetite. Defining and achieving consensus for KRIs and their thresholds, and monitoring their effectiveness, is a significant undertaking that engages business units, enterprise risk management, and internal audit. An organization’s KRI library must contain KRIs that are sufficiently high level to enable consistent measurement and guidance to the board and external stakeholders, but also sufficiently granular to provide guidance in decision making and assurance to management. Each indicator must have a forward-looking perspective, while still being based on historical data.

Furthermore, when determining an accurate measurement for a complex, or enterprise-wide risk, it is difficult to identify a single KRI that measures that risk. Having a diverse KRI library can assist in the process of deconstructing enterprise-wide risks and identifying the KRIs that drive that risk.

This white paper describes how an organization can define IT KRIs and establish KRI thresholds that align with the organization’s business objectives and risk appetite.
Risk appetite is the aggregate level and types of risk the board and management are willing to assume to achieve their strategic objectives and business plan.

The requirement for businesses to quantify risk appetite applies across industries and geographies, but regulators are particularly focused on the banking industry.

According to a ruling proposed by the OCC,1 “… the CEO should develop a written strategic plan with input from front line units, independent risk management, and internal audit.” This plan “should contain a comprehensive assessment of risks that currently impact the Bank or that could impact the Bank.” The Bank should have a “comprehensive written statement that articulates the Bank’s risk appetite.”

A 2013 Economist Intelligence Unit survey sponsored by KPMG explored how effectively companies are integrating a holistic governance, risk, and compliance (GRC) framework throughout the enterprise.2 Results of this survey showed that “…less than a fifth (19 percent) of companies has developed a formal risk appetite statement. A further 22 percent say an appetite statement is being developed. About 40 percent say that a statement has been created, but not communicated across the organization. And 19 percent say it has not been developed at all. These statistics show that there has been some progress in creating risk appetite statements, but organizations need to try harder to develop these statements for decision-making.”

The survey report concluded that when “used strategically, risk appetite frameworks can allow companies to balance their strategic ambitions with performance metrics expected by stakeholders—if a company operates without a risk appetite statement, it is hard to know whether it is taking excessive risks or too few—the latter can be as injurious as the former.”

---

Strategic view of KRIIs and why they are relevant

KRIIs play a vital role in establishing and measuring risk appetite. The purpose of KRIIs is to help shape the risk culture of the IT organization and support allocation of capital and personnel to fulfill the organization’s business objectives. An optimal KRI program should not only align with the organization’s business objectives, but also to its risk appetite.

An optimal KRI program should not only align with the organization’s business objectives, but also to its risk appetite.

Organizational alignment
Current risk management practices follow a “three lines of defense” approach. The first line is the organization’s core business processes and information technology function. The second is an enterprise risk management function (and often a dedicated IT risk management function), which monitors business processes to detect risks that may impact business goals. The third line of defense is the organization’s internal audit department. Internal audit provides assurance that the first and second layers of defense are mitigating risks to acceptable levels.

Appropriate organizational alignment for the definition and monitoring of KRIIs provides assurance that KRIIs align with the organization’s business goals and risk appetite.

The responsibility for the definition and monitoring of KRIIs should follow the same hierarchy as other risk management practices. These roles and responsibilities are shown in the graphic below:
Provide independent assurance that risks are being mitigated in accordance with organizational standards.

Set thresholds
- Monitor thresholds
- Identify patterns and risks

Provide KRI data
- Decision based on KRI data and thresholds identified by Risk Management

**KRI process**

**KRIs as a measurement**

Methods of measuring risk can range from qualitative expert observations to historical analysis to complex models leveraging automated data collection and analytics. Whichever approach is adopted, the KRIs, if appropriately articulated and benchmarked, provide management with prospective risk insights and support the consistent allocation of resources based on risk.

In order to provide an effective view of the relationship between risks and business goals, KRIs are typically built on a balanced mix of both quantitative and qualitative measures. Quantitative measures may include financial components, such as return on investment of new systems and IT project budget analysis; operational components, such as disk and CPU usage, cyber threat detection, and vendor service level agreement compliance; or traditional IT indicators, such as system uptime and number of high-severity incidents. Qualitative measures may refer to market reputation, innovation track record, customer satisfaction, and regulatory compliance.

Qualitative KRIs are inherently more difficult to measure. However, they are essential to understanding the organization’s risk position, and can be presented and analyzed as articulated trends, stoplight/color status, or rank order, among others.

**Embedding KRIs in the decision-making process**

Once defined, organizations are challenged with embedding KRIs in the decision-making process and implementing a robust governance and reporting model to ensure that IT management and operations are in line with applicable risks and KRIs. Making KRIs an integral part of the IT planning process is essential to cascading the organization’s risk appetite.
KRI development starts by identifying risk categories that could impact the organization’s operational and financial goals, as well as regulatory compliance. In Control Objectives for Information and Related Technology 5, ISACA defined three IT risk categories. Identifying risk categories assists in gaining an understanding of broad risks, establishing accountability, and aligning KRIIs with organizational structure. KPMG expanded on these three risk categories to build on the advantages of risk categories.

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Includes risks related, but not limited to:</th>
<th>Ownership/Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party management</td>
<td>Service providers, SLA monitoring, Contract compliance</td>
<td>Line of business relationship owners, Vendor Management department</td>
</tr>
<tr>
<td>Program, project, and change management</td>
<td>Change management, Project management, SDLC</td>
<td>IT application owners, Project management office, IT Infrastructure</td>
</tr>
<tr>
<td>IT operations</td>
<td>Job scheduling and processing, Backup of business data, Datacenter operations</td>
<td>IT Infrastructure</td>
</tr>
<tr>
<td>IT security</td>
<td>Malware events, Network attacks, Social engineering</td>
<td>Information Security</td>
</tr>
<tr>
<td>Data governance</td>
<td>Data classification standards, Data quality standards, Data integrity standards</td>
<td>Information Security, Line of business</td>
</tr>
<tr>
<td>IT strategy and governance</td>
<td>Capacity management, Budgeting, Audit issues</td>
<td>IT Infrastructure</td>
</tr>
<tr>
<td>Identity and access Management</td>
<td>User modifications, User terminations, Segregation of duties</td>
<td>Line of business, Information Security/IAM team</td>
</tr>
<tr>
<td>Business continuity</td>
<td>Disaster recover, Datacenter environmental controls, Testing of DR/BR plans</td>
<td>IT Infrastructure, Line of business, Business Continuity team</td>
</tr>
<tr>
<td>IT service management</td>
<td>Application uptime, Problem tickets, Inventory management</td>
<td>IT Infrastructure, Business continuity, Line of business, IT application support</td>
</tr>
</tbody>
</table>

---

3 ISACA is an independent, nonprofit, global association, comprised of a broad range of IT governance professionals
A KRI can apply to more than one risk category, and for each risk category, multiple KRIs can be defined. Ownership should be defined for each risk category and KRI. Identifying an owner for each risk category and KRI establishes accountability for the risks shown by the risk categories and KRIs.

ISACA defines KRIs as “metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.”

### Defining KRIs and thresholds
ISACA\(^4\) defines KRIs as “metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.”\(^5\) A KRI is a specific, measurable, quantitative or qualitative metric that is tied to a process, procedure, or control. The indicator should clearly characterize the point-in-time risk associated with the process, procedure, or control to which the indicator is tied. The value of any KRI should be determined using business or IT data derived from ongoing operational activity, rather than subjective opinion.

### Example KRI
A business line was considering a modification to a particular application and was concerned about the effectiveness of such changes. After consulting with risk management, the business line identified a KRI to measure the short-term effectiveness of changes to the application. By determining an optimal KRI, the business was able to measure the risk of a change to the application being ineffective.

<table>
<thead>
<tr>
<th>KRI</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Changes made to business applications were found to be useful to users&quot;</td>
<td>KRI should include qualitative data, but the data must be definitive. This is not a reasonable metric to track because it does not correlate to a specific process, procedure, or control.</td>
</tr>
<tr>
<td>&quot;Number of incidents for an application with a production change within the last 30 days&quot;</td>
<td>This is a reasonable metric because it allows management to track a specific application, for a specific process. Having this correlation allows the business to measure the short-term effectiveness of changes and determine if a new change would meet the organization’s risk appetite.</td>
</tr>
</tbody>
</table>

---


After identifying the KRI, indicative metrics, and stakeholders, each risk indicator should be benchmarked to establish a threshold. Thresholds should be set in accordance with the organization’s risk appetite. Stakeholders should be able to base specific risk responses on a single KRI’s thresholds, or through the thresholds of an aggregated set of KRI, by performing stress or what-if testing. Finally, KRI and thresholds should be monitored and analyzed to determine if they are adequately measuring and displaying risk. This process and commonly associated owners for each step are outlined in the graphic below:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description of steps</th>
<th>Ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess broad risk areas</td>
<td>– Assess broad risk areas that would have a significant effect across business lines</td>
<td>– Enterprise Risk Management</td>
</tr>
<tr>
<td></td>
<td>– Identify the stakeholders affected by each of the broad risk categories</td>
<td></td>
</tr>
<tr>
<td>Identify KRI</td>
<td>– Identify KRI that:</td>
<td>– Business units</td>
</tr>
<tr>
<td></td>
<td>» Are indicative of impact on business</td>
<td>– Enterprise Risk Management</td>
</tr>
<tr>
<td></td>
<td>» Are reasonable to implement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>» Provide a high correlation of risk indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>» Ability to assign ownership to KRI for appropriate risk responses</td>
<td></td>
</tr>
<tr>
<td>Establish KRI thresholds</td>
<td>– Provide an early warning of significant risks</td>
<td>– Enterprise Risk Management</td>
</tr>
<tr>
<td></td>
<td>– Assist in the identification of a root cause and response by the KRI’s owner</td>
<td></td>
</tr>
<tr>
<td>Monitor and analyze</td>
<td>– Monitor the values of KRI based on the thresholds found</td>
<td>– Risk Management</td>
</tr>
<tr>
<td></td>
<td>– Modify thresholds when required</td>
<td>– Enterprise Risk Management and Internal Audit</td>
</tr>
<tr>
<td></td>
<td>– Identify new and remove old KRI based on the organization’s risk appetite</td>
<td></td>
</tr>
</tbody>
</table>
Applying KRIIs to anticipate future risks

KPMG LLP’s (KPMG) IT Risk Management engagements have shown that organizations across the healthcare, oil and gas, and banking industries are beginning to focus on efforts to construct tailored IT Risk Management capabilities. However, aligning these capabilities with the organization’s enterprise risk management program and risk appetite remains a challenge.

Identifying KRIIs and calibrating thresholds that align with the organization’s risk appetite provides management with one way of monitoring IT risks facing the organization. Having this knowledge provides management with the ability to make informed business decisions that consider risks to the IT environment.

Case study
A midsize regional bank was looking to better correlate IT risk with enterprise-wide business risk. The bank had already developed an enterprise risk appetite with financial/business risk in mind. However, it had not taken into account its exposure to IT risk. The bank engaged KPMG to assist in developing a plan to better measure IT risk with the goal of incorporating IT risk into the future determination of enterprise risk appetite and evaluating IT’s alignment with enterprise risk appetite.

KPMG worked with the client to identify risk categories and implement a wide-ranging KRI library. KPMG first analyzed the primary risk categories that the client was facing compared to industry practices, and developed a set of KRIIs for measuring IT risk exposure. For each KRII, KPMG calibrated thresholds to help ensure that the enterprise risk appetite was reflected in the metrics being reported. Finally, KPMG assisted with interpretation of the KRII measurement results, and advised on the overall business impact of the reported metrics.

As a result of the engagement, the bank is now able to identify areas of heightened IT risk and focus resources in a more targeted fashion towards high-impact risk management activities. Management has implemented an effective process for producing reports that provide valuable insights for monitoring and taking action on critical areas of IT risk. In addition, management is able to easily incorporate IT risks into the determination of enterprise risk appetite.
Conclusion

Organizations should continue prioritizing IT risk management to address concerns of both regulators and stakeholders. Identifying KRIs and thresholds allows the IT risk management function to better monitor IT-related risks affecting business functions. Having these monitoring capabilities allows management to identify and understand IT risks that will have a direct impact on business activities.

Through industry diverse experience in IT risk management, KPMG has developed a standardized set of broad IT risk categories and a library of KRIs that impact each of these broad risks. By leveraging this type of library, management can accelerate the organization’s understanding of the IT risks that stand the greatest chance of affecting the organization.

About KPMG
KPMG LLP, the audit, tax and advisory firm, is the U.S. member firm of KPMG International Cooperative ("KPMG International"). KPMG is a global network of professional firms providing Audit, Tax and Advisory services. We operate in 155 countries and have more than 174,000 people working in member firms around the world.
Contact us

To learn more about ITRM, contact one of the following KPMG professionals:

David DiCristofaro  
Global Lead,  
IT Advisory in Risk Consulting  
KPMG LLP  
T: 212-872-3382  
E: ddcristofaro@kpmg.com

Vivek Mehta  
Managing Director,  
Emerging Technology Risk  
KPMG LLP  
T: 212-872-6548  
E: vivekmehta@kpmg.com

Phillip J. Lageschulte  
Network Leader,  
Emerging Technology Risk  
KPMG LLP  
T: 312-665-5380  
E: pjlageschulte@kpmg.com

Kiran Nagaraj  
Director,  
Emerging Technology Risk  
KPMG LLP  
T: 212-872-3056  
E: kirannagaraj@kpmg.com

Deon Minnaar  
Partner, Advisory  
KPMG LLP  
T: 212-872-5634  
E: deonminnaar@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 570710